



AP33088-070457.0985

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

**On Appeal to the Board of  
Appeals and Interferences**

Appellant(s) : Edward J. Hogan, *et al.* Examiner : Calvin L. Hewitt II  
Serial No. : 09/809,367 Group Art Unit: 3621  
Filed : Mar. 15, 2001  
Title : METHOD AND SYSTEM FOR SECURE PAYMENTS  
OVER A COMPUTER NETWORK

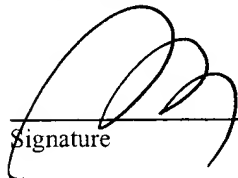
**APPEAL BRIEF**

**CERTIFICATE OF MAILING**

I hereby certify that this paper is being deposited with the United States  
Postal Service as first class mail in an envelope addressed to:  
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-  
1450 on: October 4, 2006  
Date of Deposit

Robert C. Scheinfeld  
Attorney Name

31,300  
Patent Office Registration No.

  
Signature

October 4, 2006  
Date of Signature

**TABLE OF CONTENTS**

I.	REAL PARTY IN INTEREST .....	3
II.	RELATED APPEALS AND INTERFERENCES.....	4
III.	STATUS OF CLAIMS .....	5
IV.	STATUS OF AMENDMENTS .....	6
V.	SUMMARY OF CLAIMED SUBJECT MATTER .....	7
VI.	GROUND FOR REJECTION TO BE REVIEWED ON APPEAL.....	8
VII.	ARGUMENT .....	9
VIII.	CLAIMS APPENDIX.....	15
IX.	EVIDENCE APPENDIX.....	19
X.	RELATED PROCEEDINGS APPENDIX .....	20



AP33088-070457.0985

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

**On Appeal to the Board of  
Appeals and Interferences**

Appellant(s) : Edward J. Hogan, *et al.* Examiner : Calvin L. Hewitt II  
Serial No. : 09/809,367 Group Art Unit: 3621  
Filed : Mar. 15, 2001  
Title : METHOD AND SYSTEM FOR SECURE PAYMENTS  
OVER A COMPUTER NETWORK

**APPEAL BRIEF**

Commissioner for Patents  
U.S. Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

On April 4, 2006, Appellants filed a Notice of Appeal from the final rejection of twice-rejected claims 1-10 contained in the Office Action dated October 25, 2005. The Notice of Appeal was received by the U.S. Patent and Trademark Office on Oct. 4, 2005.

10/10/2006 HGUTEMA1 00000004 09809367

01 FC:1402

500.00 OP

Applicants hereby submit, pursuant to 37 C.F.R. § 41.37, an Appeal Brief in support of the appeal of the rejections of pending claims 1-10 and a check to cover the fee for a four-month extension.

**I. REAL PARTY IN INTEREST**

The real party in interest is MasterCard International Incorporated, 2000 Purchase Street, Purchase, New York 10577-2509 ("MasterCard"). MasterCard is the assignee of the entire right, title, and interest in the present application by way of Assignments with execution dates of November 27, 2000 and December 4, 2000, which were recorded on Feb. 1, 2001 at Reel 011500 and Frame 0816.

**II. RELATED APPEALS AND INTERFERENCES**

There are no related appeals or interferences.

**III. STATUS OF CLAIMS**

Claims 1-10 stand finally rejected and are the subject of this appeal.

**IV. STATUS OF AMENDMENTS**

Appellants have not submitted after-final amendments.



**V. SUMMARY OF CLAIMED SUBJECT MATTER**

Independent claim 1 recites a method of conducting a transaction by a purchaser over a communications network (page 5, paragraph [0019]) comprising (a) assigning to said purchaser a first payment account number having a status which changes over time (page 3, paragraph [0007]); (b) providing a second payment account number associated with said first payment account number, said second payment account number being reusable by the purchaser for as long as the first payment account number is usable by the purchaser (page 3, paragraphs [0006]-[0008]), and having an encryption key assigned thereto (page 3, paragraph [0008]); (c) requesting authorization for payment of said transaction with said second payment account number and not said first payment account number (page 3, paragraph [0007]; pages 5-10, paragraph [0020]; pages 22-23, paragraphs [0028]-[0029]); (d) identifying said purchaser's first payment account number in response to said authorization request (pages 20-22, paragraph [0027]); and (e) responding to said authorization request based upon said status of said first payment account number at the time of the transaction (page 22, paragraph [0027]).

**VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL**

The grounds of rejection for review are:

(1) the rejection of claims 1-10 under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement in that the claims allegedly recite subject matter that is not supported by the specification;

(2) the rejection of claims 1-10 under 35 U.S.C. § 112, second paragraph, as being allegedly indefinite;

(3) the rejection of claims 1-7, 9 and 10 as being allegedly obvious over U.S. Patent No. 6,163,771 to Walker *et al.* (“Walker”) in view of U.S. Patent No. 6,636,833 to Flitcroft, *et al.* (“Flitcroft”); and

(4) the rejection of claim 8 as being allegedly obvious over Walker in view of Flitcroft, and further in view of U.S. Patent No. 6,018,717 to Lee, *et al.* (“Lee”).

## VII. ARGUMENT

Claims 1 through 10 stand rejected by the Examiner under both the first and second paragraphs of 35 U.S.C. § 112, for allegedly (i) failing to comply with the written description requirement, and (ii) being indefinite. In addition, the Examiner rejected Claims 1 through 7, 9 and 10 under 35 U.S.C. § 103(a) as allegedly being obvious over U.S. Patent 6,163,771 to Walker, *et al* (“Walker”) in view of U.S. Patent 6,636,833 to Flitcroft, *et al.* (“Flitcroft”). Finally, the Examiner rejected Claim 8 under 35 U.S.C. § 103(a) as allegedly being obvious over Walker in view of Flitcroft, and further in view of U.S. Patent 6,018,717 to Lee, *et al.* (“Lee”).

Applicants respectfully submit that for the reasons set forth in greater detail below the rejections were improper and should be reversed.

### I. Rejection of Claims 1-10 Under Section 112, First Paragraph

The Examiner has asserted that Claims 1 through 10 fail to meet the written description requirement of Section 112, first paragraph, because the limitation that a second payment account number (Claims 1-3) or a pseudo account number (Claims 4-10) be “reusable by the purchaser for as long as the first payment account number is usable by the purchaser,” is allegedly not supported by the Specification. According to the Examiner, one of ordinary skill in the art knows that if the pseudo number described in the Specification were to be compromised, a new pseudo number would be generated that renders the old one obsolete. *See* Office Action at pp. 2-3. Thus, reasons the Examiner, the Specification does not contain a description of a pseudo account number that is reusable for as long as the first payment account number is usable, but rather of one that is only reusable for as long as it has not been compromised.

Applicants respectfully submit that the Examiner's reasoning is flawed, and the rejection improper. A rejection under Section 112, first paragraph, is appropriate only if the Specification fails to provide an adequate description of what is claimed. This is certainly not the case here. Claims 1 through 10 recited either a second payment or pseudo account number that is reusable by the purchaser for as long as the purchaser's first payment account number is usable – a limitation which the Specification more than adequately describes. *See, e.g.*, Specification, para. [0006]-[0008] (“According to the present invention, a ‘pseudo’ account number is assigned to a customer and cryptographically linked to a consumer's payment account number . . . . The pseudo account number is used by the customer instead of the real account number for all of his or her on-line financial transactions.”).

Nowhere does the Specification state that the pseudo account number would be reusable only to the extent that it is not compromised. To the contrary, in discussing the possibility of a compromised pseudo account number, the Specification states that “if unauthorized persons were to ascertain any pseudo account numbers, they would be unable to make fraudulent transactions using them” due to the cryptographic security protecting those numbers. *See, e.g.*, Specification at para. [0008]. That is to say, the Specification actually suggests that even a compromised pseudo account number would be reusable for as long as the “real” payment account number is usable.

For at least these reasons, Applicants respectfully submit that the Examiner's rejection under Section 112, paragraph one, is without foundation, and should be reversed.

## II. Rejection of Claims 1-10 Under Section 112, Second Paragraph

The Examiner further asserts that Claims 1 through 10 are indefinite under Section 112, second paragraph, because while the Claims recite requesting authorization for payment of a transaction with the second payment *or* pseudo account number, the Specification allegedly “clearly details *authenticating* a user transaction using both a real *and* pseudo account number (Specification, figures 4a and 4, paragraph [0027]).” *See* Office Action at p. 3 (emphasis supplied). Applicants respectfully submit that this rejection is also without foundation.

First, Applicants note that it is simply incorrect that the Specification describes “authenticating” a user transaction using both real and pseudo account numbers. Both the Specification and the pending Claims describe, not “authentication,” but “authorization.” This error alone renders the Examiner’s rejection improper.

In addition, however, the Specification does not at all state, either in the portion cited by the Examiner or elsewhere, that either a pseudo or a real account number may be used to request authorization for payment of a transaction. To the contrary, the Specification clearly states that authorization requests are made using only the pseudo account number. *See* Specification at para. [0027], pp. 20-21 (“The merchant may approve the transaction *without* authorization if that is its practice or it may pass the pseudo account number and card expiration date to the acquiring bank . . . . The acquirer receiving the authorization request from the merchant recognizes that it contains a pseudo account number . . . and sends to its MasterCard-provided security module the pseudo account number . . . Upon receipt of this data, the security module cryptographically

processes the pseudo account number to produce the “real” account number as described above with reference to Fig. 3b. (The translation is shown in Figs. 4a and 4b as using function ‘D1’.)”)

The Applicants respectfully submit that the Examiner’s rejection under Section 112, second paragraph, was also improper and should be reversed.

### III. Rejection of Claims 1-7, 9 and 10 Under Section 103

In rejecting Claims 1-7, 9 and 10, the Examiner relies on the combination of Walker and Flitcroft. However, Claims 1-3 as currently amended require:

(b) providing a second payment account number associated with said first payment account number, ***said second payment account number being reusable by the purchaser for as long as the first payment account number is usable by the purchaser***, and not being a transaction number and having an encryption key assigned thereto . . .

Similarly, Claims 4-7, 9 and 10 require:

(b) providing said purchaser with a secure payment application which includes a cryptographic key that is unique to said account number and a pseudo account number, said pseudo account number having the same length as and associated with said first payment account number, and ***said pseudo account number being reusable by the purchaser for as long as the first payment account number is usable by the purchaser*** . . .

Neither Walker nor Flitcroft discloses or suggests a second payment account number or pseudo account number that is both reusable and that may be used for as long as the first payment account is usable. As the Examiner himself states, Walker does not disclose either a second payment account number or a pseudo account number that is *reusable*. See Office Action at p. 6. Consequently, Walker also fails to disclose a second payment account number or a pseudo account number that is reusable for as long as the first payment account is usable by the purchaser.

Flitcroft does not cure this deficiency in Walker. Flitcroft, as the Examiner himself states, discloses reusable “limited-use card numbers.” *See* Office Action at p. 6. In Flitcroft, a “limited-use card number” is associated with a “master credit card number.” For security reasons, a “master credit card holder” may use a “limited-use card number” instead of his “master credit card number” to complete an electronic commerce transaction. The “limited-use card numbers are either “designated for a single use . . . [or] designated for multiple uses providing that the charges accrued do not exceed a prescribed threshold or thresholds, such [as] a total single charge, total charges over a limited period, total charge in a single transaction, etc.” Flitcroft refers to these conditions as “use-triggered conditions.” That is to say, the reusability of “limited use card number” in Flitcroft depends on “use-triggered conditions” that are triggered by use of the limited use card number” itself. There is nothing in Flitcroft that discloses or suggests that the “limited use card number” is reusable for as long as the “master credit card number” is usable.

In short, neither Walker nor Flitcroft disclose a second payment account number or pseudo account number that is both reusable and that may be used for as long as the first payment account is usable. For at least this reason, the final rejection of Claims 1-7, 9 and 10 should be reversed.

#### **IV. Rejection of Claim 8**

Claim 8 was rejected as being obvious over the combination of Walker and Flitcroft, and further in view of Lee.

Claim 8, which depends from Claim 4, also requires a pseudo account number that is both reusable and that may be used for as long as the first payment account is usable. As was

previously explained in Section I, *supra*, the combination Walker and Flitcroft neither discloses or suggests this limitation. And Lee was not cited by the Examiner for the purpose of disclosing this missing limitation. Rather, Lee was cited as disclosing a method for performing secure transactions using card unique certificates that are associated with a public key of a public/private key pair. *See* Office Action, at p. 7-8. Assuming, without conceding, that this is what Lee in fact discloses, the combination of Walker, Flitcroft and Lee remains deficient with respect to Claim 8 because it fails to disclose or suggest a pseudo account number that is both reusable and that may be used for as long as the first payment account is usable. Thus, the final rejection of Claim 8 should be reversed as well.



**VIII. CLAIMS APPENDIX**

**The following claims are the subject of this appeal:**

**1. (Rejected):** A method of conducting a transaction by a purchaser over a communications network, comprising:

(a) assigning to said purchaser a first payment account number having a status which changes over time;

(b) providing a second payment account number associated with said first payment account number, said second payment account number being reusable by the purchaser for as long as the first payment account number is usable by the purchaser, and not being a transaction number and having an encryption key assigned thereto;

(c) requesting authorization for payment of said transaction with said second payment account number and not said first payment account number;

(d) identifying said purchaser's first payment account number in response to said authorization request; and

(e) responding to said authorization request based upon said status of said first payment account number at the time of the transaction.

**2. (Rejected):** The method of Claim 1, wherein said authorization request includes a cryptographic code based on said encryption key, and wherein said response to said authorization request is further based on said cryptographic code.

**3. (Rejected):** The method of Claim 2, wherein said status is a function of the credit balance available for use by said purchaser, which credit balance changes over time as a result of the purchases made by the purchaser.

**4. (Rejected):** A method of conducting a transaction by a purchaser over a communications network, comprising:

- (a) assigning to said purchaser a first payment account number having a status which changes over time;

- (b) providing said purchaser with a secure payment application which includes a cryptographic key that is unique to said account number and a pseudo account number, said pseudo account number having the same length as and associated with said first payment account number, and said pseudo account number being reusable by the purchaser for as long as the first payment account number is usable by the purchaser;

- (c) providing said purchaser with merchant data based on the transaction;

- (d) generating a message authentication code as a function of at least said merchant data and said cryptographic key;

- (e) providing said merchant said pseudo account number and said message authentication code and not said first payment account number;

- (f) verifying that said merchant data is the correct data for the transaction;

- (g) requesting an authorization for payment of said transaction, said authorization request not including said first payment account number but including said pseudo account number;

(h) recognizing said pseudo account number and cryptographically processing said pseudo account number to produce said first payment account number; and

(i) responding to said authorization request based on the status of said first payment account number, and passing said response back without transmission of said first payment account number.

**5. (Rejected):** The method of Claim 4 wherein said pseudo account number is indicated to be different from said first payment account number by a special identifier within the pseudo account number.

**6. (Rejected):** The method of Claim 4 wherein said pseudo account number is indicated to be such by data within a transaction record.

**7. (Rejected):** The method of Claim 4 wherein said cryptographic key is a secret key.

**8. (Rejected):** The method of Claim 4 wherein said cryptographic key is a private key and said secure payment application further includes a card-unique certificate for the a corresponding public key and said message authentication code comprises a digital signature generated by said secure payment application.

**9. (Rejected):** The method of Claim 4 wherein said pseudo account number is obtained by encrypting the associated first payment account number utilizing DESX methodology.

**10. (Rejected):** The method of Claim 4 wherein said pseudo account number is converted back into its associated first payment account number utilizing DEA with a double-length key.

**IX. EVIDENCE APPENDIX**

None.

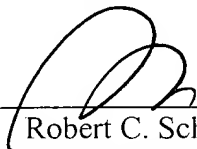
X. **RELATED PROCEEDINGS APPENDIX**

None.

For the foregoing reasons, the examiner's rejection of claims 2-11 should  
be reversed.

Respectfully submitted,

Dated: 10/4/16

By:   
Robert C. Scheinfeld  
Patent Office Reg. No. 31,300

*Attorney for Appellants*  
Telephone: (212) 408-2500

Baker Botts L.L.P.  
30 Rockefeller Plaza  
New York, NY 10112